

Approved: _____

JANE CHONG

Assistant United States Attorney

Before: THE HONORABLE GABRIEL W. GORENSTEIN
United States Magistrate Judge
Southern District of New York

-----X	:	21 MAG 11949
	:	
UNITED STATES OF AMERICA	:	<u>SEALED COMPLAINT</u>
	:	
-v.-	:	Violations of 18 U.S.C.
	:	§§ 2252A(a) (2) (B),
BRANDON CHRISTOPHER JONES,	:	(a) (5) (B) and (b) (2),
	:	and 2
Defendant.	:	
	:	COUNTY OF OFFENSE:
-----X	:	NEW YORK
	:	

SOUTHERN DISTRICT OF NEW YORK, ss.:

THOMAS THOMPSON, being duly sworn, deposes and says that he is a Special Agent with the Federal Bureau of Investigation ("FBI"), and charges as follows:

COUNT ONE
(Receipt of Child Pornography)

1. In or about May 2021, in the Southern District of New York and elsewhere, BRANDON CHRISTOPHER JONES, the defendant, knowingly received and attempted to receive material that contains child pornography that has been mailed, and using a means and facility of interstate and foreign commerce shipped and transported in and affecting interstate and foreign commerce by any means, including by computer, to wit, JONES received files containing sexually explicit images of a minor on a computer in New York, New York via a Peer-to-Peer networking program.

(Title 18, United States Code, Sections 2252A(a) (2) (B) and 2.)

COUNT TWO
(Possession of Child Pornography)

2. On or about September 23, 2021, in the Southern

District of New York and elsewhere, BRANDON CHRISTOPHER JONES, the defendant, knowingly possessed and accessed with intent to view a book, magazine, periodical, film, videotape, computer disk, and other material that contained an image of child pornography that had been mailed, shipped and transported using a means and facility of interstate and foreign commerce and in and affecting interstate and foreign commerce by any means, including by computer, and that was produced using materials that had been mailed, shipped and transported in and affecting interstate and foreign commerce by any means, including by computer, to wit, JONES possessed sexually explicit images of minors, including images of prepubescent minors and minors who had not attained 12 years of age, in his residence in New York, New York.

(Title 18, United States Code, Sections 2252A(a)(5)(B), (b)(2) and 2.)

The bases for my knowledge and the foregoing charges are, in part, as follows:

3. I am a Special Agent with the FBI, and I have been a member of the Child Exploitation and Human Trafficking Task Force since 2007. As a Special Agent, I have investigated numerous violations of criminal law relating to the sexual exploitation of children.

4. I have been personally involved in the investigation of this matter, and I am familiar with the information contained in this Complaint based on my own personal participation in the investigation, my review of documents, conversations I have had with other law enforcement officers about this matter, my training and experience, and numerous discussions I have had with other law enforcement personnel concerning the creation, distribution, and proliferation of child pornography. Because this Complaint is being submitted for the limited purpose of establishing probable cause, I have not included the details of every aspect of the investigation. Where actions, conversations, and statements of others are related herein, they are related in substance and in part, except where otherwise indicated.

Overview of Peer-to-Peer ("P2P") File-Sharing Networks and the "Software"

5. From my experience as a Special Agent with the FBI, including my participation in prior investigations relating to the sexual exploitation of children, my training, experience and

advice received concerning the use of computers in criminal activity, and from my conversations with other law enforcement personnel, I have learned that P2P file-sharing is a method of communication available to Internet users through the use of special software. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the network. A user first obtains the P2P software, which can be downloaded from the Internet.

6. This case involves the use of a particular P2P software (the "Software"). From my training, experience, and discussions with other law enforcement personnel, I know the following about the Software:

a. The Software is an "open-source" platform that is available for anyone to download and use.

b. Anyone running the Software may join and access the Software's network. Each computer running the Software connects directly to other computers running the Software, which are called its "peers." When installing the Software, each user agrees to provide to the network a portion of the storage space on the user's computer hard drive, so that files uploaded by the Software's users can be distributed and stored across the network. The Software's users can upload files into the Software's network and download files from the Software's network.

c. When a user uploads a file using the Software, the Software breaks the file into pieces (called "blocks") and encrypts each block. The encrypted blocks are then distributed randomly and stored throughout the Software's network of peers. The Software also creates an index that contains a list of all of the blocks of the file and a unique key—a series of letters, numbers and special characters—that is used to download the complete file.

d. In order to download a file using the Software, a user must have the key for the file. There are a number of ways that a Software user can download a file using a key. Some examples include: (1) the "download" box on the Software's "file sharing" page; (2) the "download" box on the message board associated with the Software or other Software add-on programs; and (3) directly through the user's web browser while the user is connected to the Software's network.

e. When a user attempts to download a file via the

Software, the Software downloads the piece of the file containing the index, which provides the information required to retrieve the individual blocks for the file. The Software then requests all of the blocks for the file from the user's peers. Rather than request all of the blocks from a single peer, requests for blocks are divided up in roughly equal amounts among the user's peers. If a user's peer does not have the particular requested blocks in its storage, that peer will then divide up the request and ask its peers for blocks, and so on. For example, if User "A" has 10 peers and requests 1000 blocks for a file, roughly 100 blocks are requested from each one of User A's peers. If Peer "B" receives User A's request for 100 blocks for the file but does not have any of those blocks in its storage, Peer B forwards on the request for those blocks to Peer B's peers. If Peer B has 10 peers of its own, roughly 10 blocks are requested from each one of Peer B's peers.

f. The Software can be used to advertise and distribute images and videos of child pornography. Unlike other file-sharing systems, the Software does not provide a search function for its users whereby users can insert search terms to locate files. Therefore, a user who wishes to locate and download child pornography from the Software must identify the key associated with a particular child pornography file and then use that key to download the file.

g. Users of the Software can identify those keys for child pornography files in a number of ways. For example, "message boards" exist on the Software's network that allow users to post textual messages and engage in online discussions involving the sexual exploitation of minors. Law enforcement agents have observed message boards labeled: "pthc," "boy porn," "hussy," "pedomom," "kidfetish," "toddler_cp," "hurtcore," and "tor-childporn." Typical posts to those message boards contain text, keys of child pornography files that can be downloaded using the Software, and in some cases descriptions of the image or video file associated with those keys.

h. Users of the Software can also obtain keys of child pornography images or videos from websites that operate within the Software and that can be accessed only through the Software. Some of those websites contain images of child pornography the user can view along with keys for child pornography files. It is also possible that users may obtain keys related to child pornography images or videos directly from other users of the Software.

7. Because of the above characteristics of the Software,

in particular the method through which the Software processes and forwards requests for blocks for particular files, law enforcement agents can investigate the trafficking of child pornography using the Software. In general terms, to do so, agents use a computer running a modified version of the Software (the "Law Enforcement Computer") and connect the Law Enforcement Computer to the Software's network. When the Law Enforcement Computer receives requests from one of its peers on the network (the "Requesting Peer") for blocks for files that are known child pornography files, the Law Enforcement Computer logs information about that request, including: the Requesting Peer's IP address; the number of peers the Requesting Peer has; the Requesting Peer's unique identifier assigned by the Software (referred to as the computer's "location"); the remaining number of times a request from the Requesting Peer for the blocks may be forwarded; the date and time the Requesting Peer requested the blocks; and the digital hash value for the requested blocks. Using the information captured by the Law Enforcement Computer, agents can determine whether it is significantly more probable than not that the Requesting Peer was the original requestor of the child pornography file, as opposed to whether the Requesting Peer was merely forwarding the request for the file from another user.

The Investigation

8. From my personal involvement in this investigation, including a review of records generated by the Law Enforcement Computer running the Software, I have learned, that in or about May 2021, a user of the Software with a particular IP address ("the IP Address") was the Requesting Peer from the Law Enforcement Computer for three known child pornography files. Based on, among other things, the total number of peers for the Requesting Peer, the total number of blocks for each of the requested child pornography videos, and the number of blocks for each of the videos requested from the Law Enforcement Computer, it was determined that the Software user at the IP Address was the original requestor of the three child pornography videos, which are described below:

a. The first file, pieces of which were requested by the IP Address from the Law Enforcement Computer on May 6, 2021, was named "[boy+girl] 11y Jaycie + 11y Mike First Time Sex (english subs).rmvb" ("File-1"). This is a video of a boy and a girl, both approximately 11 years old, engaging in oral, vaginal and anal sex.

b. The second file, pieces of which were requested by the IP Address from the Law Enforcement Computer on May 28, 2021, was named "Anya & Varia (2010) - 1290035896.wmv" ("File-2"). This is a color video depicting a naked adult male engaging in oral sex and digital penetration with two nude girls, approximately twelve and eight years old, in a bathtub.

c. A third file, pieces of which were requested by the IP Address from the Law Enforcement Computer on May 28, 2021, was named "Tara 8Yr - Ass To Mouth - February 6Th 2007.wmv.jpg" ("File-3"). This is a color image containing 20 smaller color images of an adult male engaging in oral and anal sex with a prepubescent female, approximately eight years old. I know from my involvement in other investigations that this is a confirmed minor victim.

9. From records obtained from the internet service provider for the IP Address, I know that the subscriber for the IP Address is "Brandon Jones." The physical address associated with the IP Address is the home address of BRANDON CHRISTOPHER JONES, the defendant, in New York, New York (the "Residence").

10. On or about September 23, 2021, during a search of the Residence, pursuant to a search warrant, I and other agents seized numerous electronic devices from the Residence, including computers, laptop computers, and USB thumb drives. One of the laptop computers recovered was a Dell laptop computer ("the Dell Laptop") that was found on a desk in the living room. During the search, BRANDON CHRISTOPHER JONES, the defendant, and his wife were present at the Residence, and JONES's wife identified the Dell Laptop as belonging to JONES.

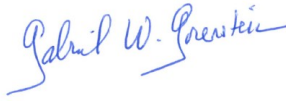
11. Based on my review of reports from the forensic examination of the Dell Laptop, I know that inside the Dell Laptop were two hard drives containing at least 1,904 images and 131 videos of what appeared to be child pornography, including File-1, which was downloaded to the Dell Laptop on or about May 6, 2021; File-2, which was downloaded to the Dell Laptop on or about May 28, 2021; and File-3, which was downloaded to the Dell Laptop on or about May 28, 2021.

WHEREFORE, the deponent respectfully requests that BRANDON CHRISTOPHER JONES, the defendant, be arrested and imprisoned or bailed, as the case may be.

/s/ sworn telephonically

Thomas Thompson
Special Agent
Federal Bureau of Investigation

Sworn to before me by reliable
electronic means pursuant to Fed.
R. Cr. P. 41(d)(3) and 4.1 this
14th day of December, 2021



THE HONORABLE GABRIEL W. GORENSTEIN
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK